Agricultural Research Service

Recommended Best Practices for Information Technology (IT) Security

(For ARS Computer Users)

Office of the Chief Information Officer
August 2001

Recommended Best Practices for Information Technology (IT) Security
(For ARS Computer Users)

Introduction

Computer information systems are increasingly an integral part of program and administrative activities throughout ARS. Virtually all ARS employees have PCs on their desktops and most are connected to the Internet and Local/Wide Area Networks (LAN/WAN). This technology and connectivity has enabled users to better access and share information throughout ARS and the agricultural community. However, it has also increased the need for heightened awareness of our system vulnerabilities, proper use of IT resources, and legal implication of information exchanges.

In a broader sense, the best-practice IT security measures presented here address:

- Appropriate Use of Information Technology Resources
- Physical Protection of Computer Hardware, Software, and Media
- Passwords Management
- Prevention of Unauthorized System Access
- Backup of Files and Data
- Work at Alternate Site
- Work while in Travel Status

Establishing and maintaining adequate security measures is critical not only to protect data and resources resident on your computer (desktop PC, laptop, palm pilot, etc.), but also to prevent unauthorized access to Agency data, systems and resources resident on centralized databases or file servers using your computer's Internet or network connection as a "back door". Sound security practices are also very important while working at home or at satellite work sites. Particularly at home where your personal computer may be used by you for official business and by other family members for personal matters, the risk of inadvertent loss or compromise of sensitive files or applications is ever present.

While many of the computer security issues we face are increasingly sophisticated and complex, they can be effectively addressed by following a few very simple Best Practices as described below.

Appropriate Use of Information Technology Resources

- Use IT resources, including the Internet and Email, for authorized purposes only as prescribed in P&P 253.4, Use of Information Technology Resources. Participating in chain letters or chat rooms; downloading games, files or programs; and accessing inappropriate or questionable web sites all increase the potential that

viruses, “Trojan Horse” programs, or other malicious files or programs will be loaded on your PC and network.

- Use caution when downloading any shareware or freeware from the Internet or bulletin board. Software obtained from bulletin boards or the Internet should be downloaded to your PC’s hard disk only if a virus scanner is in use and active. Otherwise, it should be downloaded to newly formatted diskettes and scanned for viruses before being transferred to your PC’s hard disk. All newly acquired software, regardless of source, should be scanned before installation. It is strongly recommended that you consult with management or your IT technical support staff prior to downloading any shareware or freeware from unknown or questionable sources.

- Use commercial software and shareware in accordance with licensing agreements. It is illegal to copy or distribute software or documentation without permission or a license from the copyright owner. Failure to comply with licensing agreements may result in fines or other legal action.

- Use caution when altering the configuration of Government computer equipment (other than adjusting minor user-oriented configuration settings such as your monitor display). Altering the configuration of your PC may cause conflicts between certain components of your PC resulting in system failure or loss of data. Consult with your IT technical support staff if you need any assistance with your PC configuration.

- Be wary of email file attachments sent by questionable sources. Such attachments may include viruses or other security threats. Delete such attachments or scan them for viruses before opening the file. If you have any questions about suspicious email, consult with your technical support staff for guidance and assistance.

Physical Protection of Computer Hardware, Software, and Media

- Use care when eating or drinking near computer equipment. Food and drink can easily damage computer hardware and software.

- Lock office doors (if possible) when away from the office for extended periods of time.

- Keep media containing sensitive information in locked cabinets or drawers when not in use. Disks, reports, and other media containing personnel information, database or system information, user access information, login scripts, and other sensitive data can be used to gain unauthorized access into systems or files.

- Shred, burn, or render unreadable obsolete or unneeded reports, disks, and other

media containing sensitive information (disks can be shredded once they are removed from their protective jackets). These media should not be simply thrown in the trash.

- Properly label disks, tapes, and other computer media .

- Set write-protect tabs on disks which contain software, programs, or files which you don't want to lose.

- Use virus protection software (Consult with your technical support staff for guidance and assistance on recommended virus protection tools.)

- Remove sensitive data and files from your PC prior to sending it out of the office for service.

Passwords Management

- **Passwords are the most vulnerable point of break-in for any would-be hacker. Sophisticated hackers utilize "password cracking" programs which can guess 40 percent of all passwords on a network. Establishing a good password and keeping it secure and private is the single most effective step you can take to minimize the risk of unauthorized access into your PC or network.** Utilize the following guidelines when selecting and securing your password:

  * A password should be 6 to 12 characters long, difficult to guess, but easy to remember. A password such as AX$78BO@ may be difficult to guess, but it is difficult to remember also.

  * Do not choose a password easily guessed or associated with you (i.e., your name, your name spelled backwards, dog's name, nickname, favorite team or hobby, license plate number, the word "password", etc.)

  * Use an acronym from an easy to remember phrase. "The cat in the hat ate green eggs" can translate into "TCITH8GE".

  * Use combination of letters, numbers, and symbols to construct your password. Examples:
    "L84ad8!" - late for a date
    "Uponthe^ - up on the hill
    "Iwlkth|" - I walk the line
    "fSa7yA" - Four score and seven years ago

- Change passwords a minimum of every 60 days.

- It is strongly recommended that you do not write down your password. If you use several systems which require password access thus have too many passwords to remember, establish the same one or two passwords for all the systems. When you're prompted to update one password, update them all to maintain consistency. If this is impractical and you must write down your passwords, make sure they are kept in a secure location (i.e., in an encrypted file on your PC, locked in a file cabinet, or in your wallet). Never post your passwords under your keyboard, on your monitor, in an unlocked desk drawer, or any other easy to find location.

- Do not share the password to your office PC to anyone including your supervisor, co-workers, or IT technical support staff. Files, databases, or systems which must be shared among several authorized users should be maintained on a network or shared drive. Passwords to shared PCs should only be shared among authorized users.

- If your technical support staff needs access to your system, he/she should request that you enter the password yourself. If this is impractical, you should change it immediately upon the completion of the service work.

- If it is necessary to share your password with your supervisor or co-worker for an emergency or critical purpose while your are out of the office, change your password immediately upon returning to the office.

- Change your password immediately if you suspect that your password has been compromised or someone has gained unauthorized access into your system.

Prevention of Unauthorized System Access

- Log out of your network if you plan to be away from your computer for any extended time (e.g., lunch, meeting, etc.).

- Use a password protected screensaver which invokes within 15 minutes (or other suitable timeframe) of inactivity on your PC.

- Do not leave programs or files open while away from the office for extended periods of time.

- Take appropriate steps to thoroughly clean hard drives before equipment is reassigned, surplused, or discarded. Consult with your IT technical support staff for steps to be taken.

- Be sensitive to co-workers or other persons looking over your shoulder while using your PC.

Backup of Files and Data

- Backup files and data resident on your individual PCs on a regular basis. (Consult with your technical support staff for guidance and assistance on recommended backup tools and methodology.)

- Properly label media used for backing up files and maintain in a locked and, if possible, fire-proof or off-site location.

Work at Alternate Site

- All security measures discussed above should also be considered while working at home or a satellite work site.

- If available, obtain certification from authorized officials at satellite work sites indicating that the site provides adequate protection for sensitive information and that such use conforms to applicable laws or policies.

- Sensitive materials and information may only be stored at an alternate work site if they can be locked in a secure cabinet or drawer.

- Government IT resources which have been installed at home may be used for authorized purposes only.

- Use caution when exchanging files and disks between a home and office PC. These files and disks can contain viruses (especially if the home PC is also used by other family members) and should be scanned before use.

Work while in Travel Status

- If you carry a laptop computer while traveling, keep it close at hand or locked in a secure location at all times.

- Carry your laptop with you while traveling by plane or other public transportation.

- If using your laptop for work while in transit, be sensitive to fellow travelers looking over your shoulder.

For information or questions:

Bill Keen
ARS IT Security Program Manager
ARS Office of the Chief Information Officer
(301) 504-1072
bkeen@ars.usda.gov